CLAIMS

Please find below a listing of all of the pending claims. The status of each claim is set forth in parentheses. This listing will replace all prior versions, and listings, of claims in the present application.

1. (Previously Presented) A method for secure remote mirroring of network traffic, the method comprising:

receiving a data packet to be remotely mirrored by an entry device pre-configured with a mirroring destination address to which to mirror the data packet;

forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet;

encrypting a copy of the data packet to form an encrypted packet;

incrementing an identifier to indicate a position of the encrypted packet within an order of packets received by an exit device;

generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data packet, wherein the first header includes an Internet Protocol (IP) destination address corresponding to the mirroring destination address and said identifier, the second header includes a media access control (MAC) destination address, and the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet including the IP destination address; and

forwarding the encapsulated encrypted packet to an exit device associated with the mirroring destination address.

2 and 3. (Canceled)

4. (Previously Presented) The method of claim 1, further comprising:

determining the MAC destination address associated with the IP destination address;

generating and adding, as the second header, a MAC header including the MAC destination address to the IP-encapsulated packet to form a MAC data frame, wherein the MAC header includes the MAC destination address in a destination field; and

transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain.

5. (Previously Presented) The method of claim 4, wherein determining the MAC destination address comprises:

determining if a mapping of the IP destination address to the MAC destination address is stored in an address resolution protocol (ARP) cache;

if so, then retrieving the MAC destination address from the ARP cache; and

if not, then broadcasting an ARP request with the IP destination address and receiving an ARP reply with the MAC destination address.

6. (Previously Presented) The method of claim 4, wherein the IP-encapsulated encrypted packet is communicated across multiple intermediate layer 2 domains.

7. (Previously Presented) The method of claim 1, further comprising:

receiving the encapsulated encrypted packet by the exit device;

removing the headers to de-encapsulate the encrypted packet; and

decrypting the encrypted packet to re-generate the data packet; and

using said identifier to determine the position of the data packet within the order of packets received by the exit device.

8. (Original) The method of claim 7, wherein the encrypting and decrypting is performed under a public-private key encryption scheme.

9. (Original) The method of claim 8, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device.

10. (Original) The method of claim 1, further comprising:

configuring the entry device in a best effort mirroring mode to reduce head-of-line blocking.

11. (Original) The method of claim 1, further comprising:

configuring the entry device in a lossless mirroring mode to assure completeness of mirrored traffic.

12. (Original) The method of claim 1, further comprising:

truncating the data packet to reduce a size of the data packet prior to encryption thereof.

13. (Original) The method of claim 1, further comprising:

compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption thereof.

14. (Previously Presented) A networking device comprising:

a plurality of ports for receiving and transmitting packets therefrom, wherein the packets are transmitted based on original destination addresses indicated therein;

a secure remote mirroring engine configured to detect packets from a specified mirror source, to use an incrementing identifier to indicate an order of the detected packets, to encrypt copies of the detected packets, to encapsulate each of the encrypted packets by adding, to the encrypted packet, a first header which includes said identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) destination address, and to forward the encapsulated encrypted packets to a pre-configured destination address corresponding to the IP destination address by way of at least one of the ports; and

an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

15. (Canceled)

16. (Previously Presented) The networking device of claim 14, wherein the remote mirroring engine encrypts the copies of the detected packets using a public key of a public-private key pair.

17. (Previously Presented) A system for secure remote mirroring of network traffic, the system comprising:

a mirror entry device including a secure mirroring engine configured to detect packets from a specified mirror source, to use an incrementing identifier to indicate an order of the detected packets from the specified mirror source, to encrypt copies of the detected packets using an encryption module, encapsulate each of the encrypted packets by adding, to the encrypted packet, a first header which includes said identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) destination address, and to forward the encapsulated encrypted packets to a pre-configured destination corresponding to the IP destination address by way of at least one of the ports, wherein the pre-configured destination is distinct from original destinations indicated in the detected packets, and wherein the detected packets are forwarded in unencrypted form towards the original destinations; and

a mirror exit device including a secure mirroring receiver configured to detect and decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets.

18. (Original) The system of claim 17, wherein the encrypting and decrypting is performed under a public-private key encryption scheme.

19. (Original) The system of claim 18, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device.

20. (Previously Presented) A system for secure remote mirroring of network traffic, the system comprising: a mirror entry device including means to encrypt copies of the detected packets using an encryption module and to encapsulate each of the encrypted packets by adding, to the encrypted packet, a first header which includes an incrementing identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) address, wherein the IP destination address corresponds to a pre-configured destination address of a mirror exit device and the pre-configured destination is distinct from original destinations indicated in the detected packets, and wherein the detected packets are forwarded in unencrypted form towards the original destinations; and the mirror exit device including means to decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets.

21. (Previously Presented) A method for secure remote mirroring of network traffic, the method comprising:

remotely configuring an entry device with an encryption key and mirroring destination address;

remotely configuring an exit device at the mirroring destination address with a decryption key;

receiving a data packet to be mirrored by the entry device;

incrementing an identifier to indicate a position of the data packet within an order of packets mirrored by the entry device;

encrypting a copy of the data packet using the encryption key to form an encrypted packet;

generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data packet, wherein the first header includes an Internet Protocol (IP) destination address corresponding to the mirroring destination address and said identifier and the second header includes a media access control (MAC) destination address;

forwarding the data packet in unencrypted form to an original destination address indicated in the data packet; and

forwarding the encapsulated encrypted packet to the mirroring destination address of the exit device.

22. (Original) The method of claim 21, wherein the remote configuration is performed by way of SNMP.

23. (Original) The method of claim 21, wherein the remote configuration is performed by way of a secure remote protocol.